Annual 47 C.F.R. S: 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2018 covering the prior calendar year 2017

1. Date filed: February 20, 2018

2. Name of company(s) covered by this certification: Huxley Communications Cooperative

3. Form 499 Filer ID: 814653

4. Name of signatory: Gary A. Clark

5. Title of signatory: Executive VP

6. Certification:

I, Gary A. Clark, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The company has not received customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47. C.F.R. S: 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed 

Gary A. Clark, EVP

HUXLEY COMMUNICATIONS

102 N. Main Avenue
P.O. Box 36
Huxley, IA 50124

PH 515-597-2281
TF 800-231-4922
FX 515-597-2899

www.huxcomm.net

February 20, 2018

Marlene Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street SW, Ste TW-A325
Washington, D.C. 20554

RE: Certification of CPNI Filing 47 C.F.R. §:64.2009(e)

Pursuant to Section 64.2009(e) of the FCC rules, Huxley Communications Cooperative (HCCoop) hereby submits its compliance certificate and this statement explaining how the Company's operating procedures ensure compliance with these regulations.

HCCoop has CPNI procedures to keep the disclosure of confidential information and protect the security of its customer's privacy through its electronic network policies. A supervisor's approval is required before an employee has access to any electronic database of HCCoop's records. Further, HCCoop takes all reasonable efforts to maintain the security of its electronic network from invasion by unauthorized users. HCCoop has implemented the password requirement for CPNI requests into our daily interactions with customers. To further protect customer information which is not considered CPNI, HCCoop has enacted a company policy that all customers who call in to discuss their account be required to authenticate themselves using the CPNI authentication methods required by the FCC. The FCC requires CPNI information to only be released after a customer has authenticated themselves. HCCoop has procedures in place for use when a customer is unable to authenticate themselves by password or a backup question. If a customer calls in and forgets their password and is unable to answer a backup question, the customer care representative is required to either call the customer back at their number of record, inform the customer that the information will be mailed to their address of record, or request the customer come in to the office and present photo identification. These alternative authentication methods ensure that customer data remains safe from unauthorized individuals.

If a customer chooses to change information on their account or alter their services, a program within the database automatically flags that person's information and a letter is generated which is then sent out to the customer address of record prior to any changes. The letter informs the customer a change has been made to their account and a phone number is provided for them to call if they have any questions. New customers to

HCCoop are informed about CPNI and why they need to protect their information. Customers are asked to provide a CPNI password and backup authentication answers at the time the customer initiates service with the company.

HCCoop has instituted a breach notification policy which covers internet and traditional breaches. Both are taken seriously and handled expeditiously. All customer care representatives have been trained to understand the breach policy and what steps must be followed to report that breach. For a traditional breach, the representative is required to fill out a CPNI Breach Notification Form. This form contains the customer's information, the representative's information who handles the complaint, and finally a narrative of the complaint being reported. This form is then submitted to both the representative's immediate supervisor as well as the General Manager. The General Manager then takes this information and reports the breach to the local law enforcement. As soon as practicable, and in no event later than 7 days of the determination of the breach, HCCoop shall electronically notify the United States Secret Service and the Federal Bureau of Investigation through a central reporting facility. The FCC will maintain a link to the reporting facility at http://www.fcc.gov/eb/cpni. HCCoop will not notify the customer of the resolution to the breach until after law enforcement has investigated the breach and given permission to proceed with notification.

New employees are oriented on CPNI policy and procedures by attending a training session with their supervisor. Details of the CPNI policies are reviewed during the training session. Topics that are covered include: purpose, procedures, setting up or changing a verification code, scripting, customer forgetting verification code, setting up a security question and answer and when a verification code is not required. Common customer scenarios are discussed in this training. Anuual training sessions on CPNI are required for all employees that have access to CPNI information. All employees follow strict policy regarding CPNI information. All employees at HCCoop must read and acknowledge receipt of the HCCoop CPNI policy at the time of hire. The failure of an employee to observe and follow this company policy is subject to discipline, up to and including dismissal. To add an additional layer of security, HCCoop requires all employees who have access to CPNI to read and acknowledge receipt of HCCoop's CPNI policy. HCCoop policy expressly forbids the disclosure of confidential information to anyone unless preapproved by the General Manager.

HCCoop is aware that pretexters and their ability to obtain data are a major threat to customers and HCCoop has instituted all requirements by the FCC into the daily operations of the company as well as implementing procedures for protecting non-customer detail information. By instituting the different procedures explained in this statement, HCCoop believes it is doing everything in its power to protect its customers and their data.